The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
11/05/2020

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Apple Products. The most severe of these vulnerabilities could allow for arbitrary code execution.

- watchOS is a mobile operating system created & developed by Apple to be utilized by its Apple Watch product line.
- iOS is a mobile operating system created & developed by Apple to be utilized by its mobile devices such as the iPhone.
- iPadOS is a mobile operating system created & developed by Apple to be utilized by its iPad product line.
- macOS is a desktop operating system for Macintosh computers.
- tvOS is an operating system based on iOS developed for AppleTV.

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

THREAT INTELLIGENCE:
There are reports of the following vulnerabilities currently being actively exploited in the wild:

- CVE-2020-27930: FontParser vulnerability which can enable arbitrary code execution.
- CVE-2020-27950: A memory leak vulnerability in the kernel
- CVE-2020-27932: A type confusion vulnerability that enable for privilege escalation

SYSTEMS AFFECTED:

- watchOS versions prior to watchOS 7.1, watchOS 6.2.9, watchOS 5.3.9
- macOS Catalina versions prior to macOS Catalina 10.15.7
- tvOS versions prior to tvOS 14.2
- iOS versions prior to iOS 14.2
- iPadOS versions prior to iOS 14.2

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in iOS, iPadOS, watchOS, tvOS and macOS. The most severe of these vulnerabilities could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

All OS (watchOS 7.1, watchOS 6.2.9, watchOS 5.3.9, macOS Catalina 10.15.7, tvOS 14.2)

- A memory corruption issue was addressed in processing font files with improved input validation. (CVE-2020-27930)
- A memory initialization issue was addressed in the OS kernel (CVE-2020-27950)
- A type confusion issue was addressed with improved state handling in the OS kernel (CVE-2020-27932)

WatchOS 7.1, tvOS 14.2, iOS 14.2 and iPadOS 14.2

- An out-of-bounds read was addressed for audio file processing with improved input validation. (CVE-2020-27910)
- An out-of-bounds write was addressed for audio file processing with improved input validation. (CVE-2020-27916)
- An out-of-bounds write was addressed for audio file processing with improved input validation. (CVE-2020-10017)
- An out-of-bounds read was addressed for audio file processing with improved input validation. (CVE-2020-27909)
- An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. (CVE-2020-10003)
- An out-of-bounds write issue was addressed in processing font files with improved bounds checking. (CVE-2020-27927)
- A logic issue was addressed with improved state management in Foundation. (CVE-2020-10002)
- An out-of-bounds write was addressed with improved input validation in ImageIO. (CVE-2020-27912)
- A memory corruption issue was addressed with improved state management in IOAcceleratorFamily (CVE-2020-27905)
- A logic issue was addressed with improved state management in the OS kernel (CVE-2020-9974)
- A memory corruption issue was addressed with improved state management in the OS kernel (CVE-2020-10016)
- A use after free issue was addressed with improved memory management in libxml2 (CVE-2020-27917)
- An integer overflow was addressed through improved input validation in libxml2 (CVE-2020-27911)

- A path handling issue was addressed with improved validation in Logging (CVE-2020-10010)
- A use after free issue was addressed with improved memory management in WebKit (CVE-2020-27918)

iOS 14.2 and iPadOS 14.2

- An issue existed in the handling of incoming calls in CallKit. The issue was addressed with additional state checks. (CVE-2020-27925)
- A person with physical access to an iOS device may be able to access stored passwords without authentication via Keyboard. (CVE-2020-27902)
- A use after free issue was addressed with improved memory management in libxml2 (CVE-2020-27926)
- A logic issue was addressed with improved state management in model I/O (CVE-2020-10004)
- An out-of-bounds read was addressed with improved input validation in model I/O (CVE-2020-13524)
- An out-of-bounds read was addressed with improved bounds checking (CVE-2020-10011)
- A use after free issue was addressed with improved memory management (CVE-2020-27918)

iOS 12.4.9

- A logic issue existed in the handling of Group FaceTime calls. The issue was addressed with improved state management. (CVE-2020-27929)

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Apple:

https://support.apple.com/en-us/HT201222
https://support.apple.com/en-us/HT211928
https://support.apple.com/en-us/HT211929
https://support.apple.com/en-us/HT211930
https://support.apple.com/en-us/HT211940

https://support.apple.com/en-us/HT211944
https://support.apple.com/en-us/HT211945
https://support.apple.com/en-us/HT211947

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9974
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10002
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10003
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10004
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13524
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27902
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27905
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27909
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27910
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27911
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27912
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27916
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27917
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27918
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27925
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27926
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27927
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27929
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27930
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27932
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27950